John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel.: (858) 209-6941
jnelson@milberg.com

LEEDS BROWN LAW, P.C.
Brett R. Cohen (SBN 337543)
bcohen@leedsbrownlaw.com
One Old Country Rd., Ste. 347
Carle Place, NY 11514
Tel: (516) 873-9550

Attorneys for Plaintiff & the Putative Class
Additional Counsel listed on Signature Page

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

DAVID BOWER, individually and on behalf of all others similarly situated, Plaintiff, - against - LOANDEPOT, INC. and related entities, Defendant.	**Case No.:** **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiff David Bower ("Plaintiff"), individually and on behalf of all others similarly situated, by his attorneys, Leeds Brown Law, P.C., files this class action complaint against

Defendant LOANDEPOT, INC. ("Defendant"), and in support thereof alleges the following:

INTRODUCTION

1. This class action arises out of the recent data breach on Defendant's network that resulted in unauthorized access to, and disclosure of, the highly sensitive data of approximately 16.6 million individuals (the "Data Breach").[1] As a result of the Data Breach, putative Class Members like Plaintiff Bower suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, fraudulent transactions, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. Upon information and belief, the specific information compromised in the Data Breach includes, but is not limited to, personally identifiable information ("PII") exchanged in the normal course of applying for and obtaining a mortgage or other personal financing, such as full names, phone numbers, email addresses, mailing addresses, Social Security numbers, state identification numbers, and tax identification numbers.

[1] https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed February 8, 2024).

3. Upon information and belief, beginning in 2010 and up to and through the present, Defendant obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network, from which unauthorized actors used an extraction tool to retrieve sensitive PII belonging to Plaintiff and Class Members.

4. The PII of Plaintiff and Class Members was entrusted to Defendant, its officials, and agents, yet was compromised and unlawfully accessed due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated service that stored Plaintiff's and Class Members' PII.

8. Defendant's failure to safeguard its clients' PII is particularly negligent and reckless in light of the fact that Defendant suffered a prior (unrelated) data breach in August 2022, which customers were notified of in May 2023.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks associated with the unauthorized disclosure of the PII as to Plaintiff and Class Members will exist for the duration of their respective lifetimes.

10. In fact, Plaintiff Bower has already identified separate occasions in which bank accounts were fraudulently opened in his name and Defendant's breach here is the only known occasion in which his PII has been breached.

11. Defendant failed to provide timely, accurate and adequate notice to Plaintiff and Class Members. Plaintiff's and Class Members' knowledge about the PII Defendant allowed to be accessed, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

12. As remediation for allowing Plaintiff's and Class Members' PII to be acquired by an unauthorized third-party, Defendant has stated that "[t]he Company will notify [the affected] individuals and offer credit monitoring and identity protection services and no cost to them."[2] To date, Defendant has not offered any remediation, correction, or resolution to the victims of this Data Breach, but this assurance serves as an acknowledgement of the harm and elevated risk that 16.6 million individuals now face as a result of Defendant's conduct.

13. Indeed, armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names (as was done to Plaintiff Bower), taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present, heightened, and imminent risk of fraud, identity theft, and other potentially dangerous and damaging acts. Plaintiff and Class Members must now closely

[2] *Id.*

monitor their financial accounts to guard against identity theft or these risks for the immediate future and beyond – including potentially for the rest of their lives.

15. Plaintiff and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

17. Accordingly, Plaintiff brings claims on behalf of himself and the Class for: (i) negligence, (ii) invasion of privacy and (iii) unjust enrichment, (iv) violations of the California Unfair Competition Law, (v) declaratory judgment and injunctive relief, and (vi) violations of the New York Deceptive Trade Practices Act. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

18. Plaintiff Bower is a citizen of the State of New York, and at all times relevant to this action, resided and was domiciled in Niagara County, New York.

19. In or around 2010, Plaintiff Bower secured a mortgage through Defendant for the purchase of a residence in Niagara Falls, New York.

20. During 2010, Plaintiff Bower submitted confidential information and PII to Defendant to secure financing and ultimately obtain such financing.

21. Since 2010, including in the last few years, Plaintiff Bower has continued to submit confidential information and PII as needed to make his required payments and comply with his agreement with Defendant.

22. Defendant LOANDEPOT, INC. is a citizen of the State of Delaware and California. It is a company organized under the laws of the state of Delaware, and its principal place of business is located at 6561 Irvine Center Drive, Irvine, California.

JURISDICTION & VENUE

23. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than at the named Defendant.

24. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and conducts business in California and this District through its headquarters, offices, parents, and affiliates.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

26. On or around January 8, 2024, Defendant posted the following online:

> LoanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers and we are focused on resolving these matters as soon as possible.[3]

27. Over the next three weeks, Defendant supplemented this post with nine additional updates.[4]

28. To date, Defendant's investigation has determined that the private information of approximately 16.6 million customers and other affiliated individuals was accessed and compromised by an unauthorized user on or about January 8, 2024.

[3] https://loandepot.cyberincidentupdate.com/ (last accessed February 8, 2024).
[4] *Id.*

29. It is likely the Data Breach was targeted at Defendant due to its status as a financial services provider that collects, creates, and maintains sensitive PII.

30. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiff and the Class Members.

31. While Defendant stated in its public notice it would directly notify the affected individuals and that it is committed to keeping the victims informed, Defendant has not yet directly notified Plaintiff or, upon information and belief, Class Members.

32. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff further believes their PII was likely subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals.

33. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

34. In response to the Data Breach, Defendant admits it worked with third-party security experts to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

35. Because of the Data Breach, data thieves were able to gain access to Defendant's private systems on January 8, 2024, and were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.

36. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

37. Plaintiff and the Class Members reasonably relied (directly or indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

38. Plaintiff's and putative Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to its blatant failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and the putative Class will remain for their respective lifetimes.

B. Defendant's Business

39. Defendant proclaims to be the country's fifth largest retail mortgage lender and the country's second largest nonbank retail originator. Defendant currently employes more than 6,000 individuals and services more than 27,000 customers each month.[5]

40. Upon information and belief, Defendant maintains the PII of customers, employees, and others, including but not limited to, name, address, phone number and email address; date of birth; demographic information; Social Security number; tax identification number; financial information; medication information; health insurance information; photo identification; employment information; and, other information that Defendant may deem necessary to provide its services.

41. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential static PII, which can be used to commit myriad financial crimes.

42. Because of the highly sensitive and personal nature of the information Defendant acquires, stores, and has access to, Defendant, upon information and belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical

[5] https://www.loandepot.com/about (last accessed February 8, 2024).

care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

44. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

45. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

C. The Data Breach was a Foreseeable Risk and Defendant was on Notice

46. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial services industry and other industries holding significant amounts of PII preceding the date of the breach.

47. Considering some recent high profile data breaches at other financial services companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.

48. Defendant knew or should have known that these attacks were common and foreseeable.

49. Indeed, Defendant itself was subject to a separate data breach in August 2022.

50. These types of attacks are sharply on the rise. To wit, in 2023, there were a record 3,205 total compromises, which represents a 72% increase from the previous all-time high figure that was recorded in 2021.[6]

51. Therefore, the increase in such attacks, and the likely risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

D. Defendant Fails to Comply with FTC Guidelines

52. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt

[6] Identity Theft Resource Center's Annual Data Breach, available at https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last accessed February 8, 2024).

information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[7] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[8]

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third- party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[7] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed February 8, 2024).

[8] *Id.*

56. The FTC enforcement actions include actions against insurance providers and partners like Defendant.

57. Defendant failed to properly implement basic data security practices.

58. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendant was at all times fully aware of its obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Fails to Comply with Industry Standards

60. As shown above, experts studying cyber security routinely identify insurance providers and partners as being particularly vulnerable to cyberattacks because of the value of the PII which it collects and maintains.

61. Several best practices have been identified that at a minimum should be implemented by insurance providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and

anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

62. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

63. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

F. Defendant's Breach

65. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions: failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks; failing to adequately protect PII; failing to properly monitor their own data security systems for existing intrusions; failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures; failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted; failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights; failing to implement policies and procedures to prevent, detect, contain, and correct security violations; failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports; failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII; failing to train all members of their workforces effectively on the policies and procedures regarding PII; failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to

unauthorized individuals; failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; failing to adhere to industry standards for cybersecurity as discussed above; and, otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

66. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's database, which provided unauthorized actors with unsecured and unencrypted PII.

67. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

68. Cyberattacks and data breaches at financial services companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

69. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity

theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

70. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

[9] See U.S. GOV. ACCOUNTING OFFICE, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007) https://www.gao.gov/new.items/d07737.pdf (last accessed February 8, 2024).

71. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

72. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

73. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[10] See IdentityTheft.gov, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited February 8, 2024).

74. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[11]

75. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

76. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

77. PII is such a valuable commodity to identity-thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

78. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

[11] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

79. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

80. PII can sell for as much as $363 per record according to the Infosec Institute.[12] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

81. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[13] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits or apply for a job using a false identity.[14] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

[12] See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed February 8, 2024)

[13] Identity Theft and Your Social Security Number, SOCIAL SECURITY ADMINISTRATION (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed February 8, 2024).

[14] *Id.* at 4.

82. Moreover, it is not a straightforward task to change or cancel a stolen Social Security number.

83. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

84. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[16]

85. Because of the value of its collected and stored data, the financial services industry has experienced disproportionally higher numbers of data theft events than other industries.

86. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on

[15] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (February 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed February 8, 2024).

[16] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (February 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed February 8, 2024).

notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly safeguard against such risk.

H. Plaintiff's and Class Members' Damages

87. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

88. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

89. Plaintiff and Class Members' full names, addresses, tax identification numbers, and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software maintaining PII. This PII was acquired by some unauthorized, unidentified third- party threat actor.

90. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

91. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

92. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

93. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

94. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

95. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

96. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

97. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

98. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

99. Plaintiff and Class Members were also damaged via benefit-of-the- bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's systems and Plaintiff's and Class Members' PII. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

100. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and PII for misuse.

101. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to: reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims; purchasing credit monitoring and identity theft prevention; placing "freezes" and "alerts" with reporting agencies; spending time on the phone with or at financial

institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name; contacting financial institutions and closing or modifying financial accounts; and closely reviewing and monitoring Social Security numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

102. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

I. Plaintiff Bower's Experience

103. Plaintiff Bower provided his information to Defendant as a condition of applying for and/or receiving Defendant's home financing services related to his home residence located in Niagara Fall, New York, which was purchased in or around 2010 via financing from Defendant.

104. Plaintiff Bower is careful about sharing his sensitive Private Information. Plaintiff Bower has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

105. Plaintiff Bower first learned of the Data Breach after seeing a post about the Breach on social media on or about January 26, 2024.

106. Based on the information he provided to Defendant, Plaintiff Bower has come to understand that his PII including, but not limited to, his name, address, phone number, email address, Social Security number, and/or financial information were compromised in this Data Breach.

107. As a result of the Data Breach, Plaintiff Bower made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

108. Plaintiff Bower has spent significant time and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

109. Plaintiff Bower suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Bower; violation of his privacy rights; the theft of his PII; present, imminent and impending injury arising from the increased risk of identity theft and fraud; and, fraudulent activity

associated with his name and PII including fake bank accounts being opened using his PII and under his name.

110. As a result of the Data Breach, Plaintiff Bower anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

CLASS ALLEGATIONS

111. Plaintiff brings this action individually and as a class action on behalf of a proposed Class pursuant to Federal Rule of Civil Procedure 23.

112. Plaintiff proposes the following Class and Sub-Class, consisting of and defined as:

> All persons identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach. ("Class")
>
> All persons identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach, who at the time of the Data Breach or at any time they have been customers of Defendant were residents of the State of New York. ("Sub-Class")

113. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from

the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

114. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

115. Numerosity: The members of the Class are so numerous that individual joinder of all Class members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of millions of individuals whose sensitive data was compromised in the Data Breach.

116. Commonality: This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: if Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII; if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations; if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards; if Defendant owed a duty to Class Members to safeguard their PII; if Defendant breached their duty to Class Members to safeguard their PII; if Defendant knew or should have known that their data security systems and monitoring processes were deficient; if Defendant should have

discovered the Data Breach sooner; if Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct; if Defendant's conduct was negligent; if Defendant's breach implied contracts with Plaintiff and Class Members; if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members; if Defendant failed to provide notice of the Data Breach in a timely manner, and; if Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

117. Typicality: Plaintiff's claims are typical of the other Class members' claims because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

118. Adequacy of Representation: Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including consumer protection litigation. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

119. Superiority: This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision making.

120. Predominance: Common questions of law and fact predominate over any questions affecting only individual Class members. A common pattern and practice of privacy violations are the predominant question to be tried. Individual questions, if any, are relatively minor in relation to the common questions listed above.

121. Ascertainability: Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Defendant's records. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

122. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

123. Plaintiff and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

124. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

125. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system – and Class Members' PII held within it – to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

126. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

127. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

128. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

129. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

131. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following: failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII; failing to adequately monitor the security of their networks and systems; failing to have in place mitigation policies

and procedures; allowing unauthorized access to Class Members' PII; failing to detect in a timely manner that Class Members' PII had been compromised; and failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

132. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

133. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

134. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

135. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

136. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII – whether by malware or otherwise.

137. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

138. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members – which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

139. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members'

injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

140. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

141. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

142. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

143. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

144. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

145. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

146. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

147. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

148. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

149. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

150. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

151. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

152. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

153. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

154. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

155. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

156. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

157. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

158. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

159. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering insurance related services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

160. Defendant was enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid the data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

161. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

162. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

163. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

164. Plaintiff and Class Members have no adequate remedy at law.

165. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise,

publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

166. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

167. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH CAUSE OF ACTION
UNFAIR OR UNLAWFUL ACTS OR PRACTICES
CALIFORNIA BUSINESS AND PROFESSIONS CODE SECTION 17200
(On Behalf of Plaintiff and the Class)

168. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

169. Plaintiff and Class Members qualify as a "person[s]" as defined by California Business & Professions Code section 17201. California Bus. & Prof. Code section 17204 authorizes a private right of action on both an individual and representative basis.

170. California Business and Professions Code Section 17200 declares to be "unfair competition" four types of acts or practices: (1) an "unlawful" business act or practice, (2) an "unfair" business act or practice, (3) a "fraudulent" business act or practice, and (4) "unfair, deceptive, untrue or misleading advertising." Unfair competition need not qualify as all four of these types of wrong to be actionable.

171. Defendant engaged in unlawful conduct under section 17200 et seq. with respect to the services provided to the Class.

172. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment in violation of California's data

breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods for safeguarding the PII of Plaintiff and the Class Members.

173. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

174. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the products and services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

175. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

176. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, disgorgement of all profits accruing to Defendant because of its

unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

177. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

178. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

179. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

180. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: Defendant owed, and

continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act; Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

181. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e., Plaintiff and the Class's) data.

182. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

183. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

184. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

SIXTH CAUSE OF ACTION
VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
(NEW YORK GEN. BUS. LAW § 349)
(On Behalf of Plaintiff and the Sub-Class)

185. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

186. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Sub-Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Sub-Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Sub-Class by representing that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Sub-

Class Members' PII;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Sub-Class Members' PII;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Sub-Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Sub-Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

187. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiff's and the Sub-Class Members' PII entrusted to it, and that the risk of a data breach or theft was highly likely.

188. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

189. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including

Plaintiff and Sub-Class Members) regarding the security of Defendant's network and aggregation of PII.

190. The representations upon which consumers (including Plaintiff and Sub-Class Members) relied were material representations (e.g., as to Defendant's adequate protection of PII), and consumers (including Plaintiff and Sub-Class Members) relied on those representations to their detriment.

191. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Sub-Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

192. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Sub-Class Member's PII and that the risk of a data security incident was high.

193. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing employment benefit services to consumers in the State of New York.

194. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Sub-Class Members' PII was disclosed to

third parties without authorization, causing and will continue to cause Plaintiff and Sub-Class Members damages.

195. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and Sub-Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Sub-Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Sub-Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Sub-Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed Sub-Class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Sub-Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Sub-Class Members' PII.

196. As a result, Plaintiff and the Sub-Class Members have been damaged in an amount to be proven at trial.

197. Plaintiff brings this action on behalf of himself and Sub-Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Sub-Class Members, and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

198. Plaintiff and Sub-Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, in junctive relief, and/or attorney's fees and costs.

199. On behalf of himself and other members of the Sub-Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

200. Also as a direct result of Defendant's violation of GBL § 349, Plaintiff and the Sub-Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Sub-Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class Members, prays that judgment be entered against Defendant, and that Plaintiff and the Class Members be awarded monetary and other relief from Defendant, as follows:

- Certify the Class and Sub-Class as requested herein;
- Appoint Plaintiff to serve as the Class Representative for the Class and Sub-Class;
- Appoint Plaintiff's Counsel as Class Counsel in this matter;
- Award monetary relief to Plaintiff and the Class and Sub-Class;
- Enter injunctive and declaratory relief as appropriate;
- Award Plaintiff and the Class and Sub-Class pre-judgment and/or post-judgment interest as prescribed by law;
- Reasonable attorneys' fees and other litigation costs reasonably incurred on behalf of the Class and Sub-Class Members;
- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

TRIAL BY JURY

Pursuant to the Seventh Amendment to the Constitution of the United States of America, Plaintiff and Class Members are entitled to, and demand, a trial by jury.

Dated: February 13, 2024

Respectfully Submitted,

/s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel.: (858) 209-6941
jnelson@milberg.com

LEEDS BROWN LAW, P.C.
Brett R. Cohen (SBN 337543)
bcohen@leedsbrownlaw.com
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
Tel: (516) 873-9550

LEVIN SEDRAN & BERMAN LLP
Charles E. Schaffer *
cschaffer@lfsblaw.com
510 Walnut St., Ste 500
Philadelphia, PA 19106
Tel: (215) 592-1500

GOLDENBERG SCHNEIDER, LPA
Jeffrey S. Goldenberg *
Todd B. Naylor *
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com
4445 Lake Forest Dr., Ste. 490
Cincinnati, OH 45242
Tel: (513) 345-8291

Attorneys for Plaintiff & the Putative Class

** Pro hac vice forthcoming*